Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
1	Is there a way to download your IT Security/Vulnerability Assessment (2016-22-02) RFQ off of this page? http://purchasing.franklincountyohio.gov/businesses/bid-opportunities/bids.cfm?id=717. I don't see a link or perhaps you want the vendors to register first?	If after registering if you still experience difficulties, please do not hesitate to let me know.
2	For Section 3.1: Intrusion detection analysis of the FCDN, we were hoping to get some more information on what exactly the project is looking for. Do you have any more information on this specific project and scope?	At a minimum Franklin County expects the following three items along with other considerations the vendor recommends. 1. Review the architecture design and configuration of existing IDS and firewall systems. 2. Analyze log files of existing IDS and firewall systems. 3. Provide reports and their recommendation.
3	Under 3.0 Scope of Work, 3.6 states "Assessment PCI (Payment Card Industry) compliance" Does Franklin County require a PCI certified assessment, meaning does the vendor need to be either a QSA or ASV?	Franklin County will not disqualify any vendor based on credentials or certifications, however will consider them as one of the many evaluation points during the assessment.
4	In order for our team to properly scope and assess the project, we were hoping to get some more information around the types and the count of the actual IDS and firewalls. Do you have any additional information around these tools?	Franklin County uses a third party managed service provider for IDS services. One redundant firewall.
5	For 3.1 Intrusion Detection Analysis: Could you further clarify what Franklin County is looking for? Are you looking for an architecture review, configuration review or operation review?	Architecture, configuration, and operation review including log analysis.
6	How many allocated and live external IP's are in scope?	Approximately 220 external Ips.
7	For 3.3.4 Sub-Domain – Could you further clarify what Franklin County is looking for? What type of sub-domain? Are you referring to an AD forest?	It is a AD sub-domain in the same forest.
8	For 3.4.1 One Web Application – How many dynamic pages and user roles does this application have?	Six dynamic pages. No user roles.
9	For 3.4.2 One In-House Developed Windows-based application – How many active lines of code will we be testing? What language is the application written it?	VB6.
10	For 3.4.3 One third-party software application – If the third party hasn't provided attestation – we need to know if the application is web based or hosted. Do we have access to the source code?	Installed on prem and you will have access to the source code. 300 active roles. There is one web-based service - Employee Self Service which contains 10 pages.
11	For 3.4.4 One IBM iSeries integrated application – Could you further define? Do we have access to source code?	While running on the iSeries platform (backend). The front end is running on Windows. Yes, you will have access to the source code.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
12	For all of the applications in scope: Do you have a staging environment where we can test? If not, please explain.	We FCDC does have a staging environment.
13	3.5 HIPAA Assessment – Could you provide us with a business use case? What is included in scope for HIPAA?	Does our data management structure align with HIPPA standard rules.
14	3.6 PCI Assessment – Has Franklin County completed previous assessments? Do you report on compliance or conduct a self-assessment? What is included in scope for PCI?	Identify any risks within our end-to-end infrastructure engineering performing payment processing functions.
15	For 3.5 and 3.6 (HIPAA and PCI Assessment) – Are you conducting these assessment for network requirements or do you need a full audit?	Assessment for infrastructure and data requirements.
16	For 3.7.3 Forensic Analysis – We believe this ties into the work that supports 3.1 through 3.4. Please clarify or further explain if this is correct/not correct	Correct. We would like to understand the tools, techniques and findings thus are requiring the items listed.
17	Does FCDC require the Intent to Bid form be faxed or mailed along with the email copy?	Please mail eight (8) original hard copies and one blank copy of all requested documentation, including binding signatures by 2:00 p.m. January 22, 2016.
18	How would FCDC like the proposer to conduct the intrusion detection analysis?	Yes.
19	A documentation-based review of intrusion detection methods? o A live penetration test followed by an audit of whether the IDS detects our activities? o A rule set review for the equipment and software used?	Yes and yes.
20	What IDS solutions are currently in place?	Will be disclosed in detail to the selected vendor.
21	How many wireless network are in scope for this project?	One.
22	How many access points are on each wireless network?	Approximately 20.
23	How many IPs are on the internal and external networks?	Approximately 16,777,214 IP addresses available internal and 2500 available external IP addresses, not all of them are used.
24	Who owns and operates the "two-way trusted domain"? If it is not FCDC, are they aware and okay with the testing?	Yes.
25	Does FCDC want white, grey, or black box testing on the web applications? Can FCDC specify which application should undergo which type of testing?	3.4.1 Black Box. 3.4.2 White Box. 3.3.3 Black Box. 3.4.4 Black Box.
26	How many pages are on each application?	Less than 10 each.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
27	Is the third party software application in Section 3.4.3 desktop or web-based? Which type of testing would FCDC like conducted? What is the number of active web pages and web services?	All users utilize an installed PC client. 300 active roles. There is one service that is web based - ESS (Employee Self Service) this has approximately 10 pages.
28	Can FCDC describe how it wants the forensic analysis conducted? For example, does FCDC expect an after action forensic analysis of every system accessed during penetration testing? Just perimeter systems?	All selected servers conducting the penetration testing.
29	Does analysis performed during the penetration test (documenting what is performed, effect of the attacks, etc.) sufficient for the forensic analysis?	Yes.
30	Can FCDC describe the function and nature of the IBM iSeries integrated application?	Detailed information will be provided during the contract negotiation. - basically - Overall it is a read only, user based Cold Fusion website that accesses DB2 and Cobol programs on the iSeries platform.
31	What does FCDC want conducted for HIPAA compliance? Would this include a controls review? Compliance gap assessment? Risk assessment?	We are not sure, we are looking for vendor recommendations.
32	What business processes are in scope for HIPAA?	We are not sure, we are looking for vendor recommendations - basically data access, logical data controls, and County policy on data controls.
33	Is FCDC a covered entity or business associate?	Covered entity
34	What does FCDC want conducted for PCI compliance? Would this include a controls review? Compliance gap assessment? Risk assessment?	We are looking for vendor recommendations.
35	What is your timeframe for completion of this engagement?	FCDC will conduct oral presentations of the top ranked vendors 2/2/2016 - 2/8/2016, finalize a contract 2/23/2016 and the final vendor deliverable will be due 5/31/2016.
36	Has FCDC been PCI compliant in the past or is this the first attempt?	First attempt.
37	Are you currently PCI compliant?	No, this will be our first attempt. We have transferred risk of PCI compliance to our vendors, but now are looking to obtain our own compliance.
38	Who is your current PCI QSA company?	Not applicable.
39	What business processes are in scope for PCI?	Fee and Fund payments from our partner agencies. Additional details will be provided during contract negotiations.
40	Has an accurate software inventory been developed for PCI focused systems? (required for PCI)	No. Transactions per year are less than 100,000
41	Has an accurate hardware inventory been developed of all CHD systems and devices? (required for PCI)	An inventory that should be relatively available.
42	How does FCDC accept cardholder data?	Vendor official payments, Elavon, are the primary vendors.
43	How many transactions does FCDC process per year?	< 100,000 per year.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
44	Is section 3.1, are you requesting only the analysis of the perimeter or is a penetration test requested too? What are the number of assets that make up the DMZ, inside and outside perimeter? For example, how many servers and firewalls make up section 3.1?	Both perimeter and penetration test. The numbers of servers and firewalls will be disclosed in detail to the selected vendor.
45	Pertaining to section 3.2, Ethical hack and penetration testing, is the expectation to perform an internal ethical attack, and external ethical attack, or both types of attacks?	We don't expect to include internal ethical attack.
46	In section 3.2, how many IP address are in place for an internal penetration test? Are there specific systems and subnets that you would like tested? Are there specific locations/databases?	About 5-10 selected systems will be included in the scope of penetration test. Database are installed on some of those servers.
47	Is an internal penetration test of the network desired as part of this assessment in section 3.4? Is a penetration test against the wireless subnet desired as part of this assessment in section 3.4? Are telephony/ IT phones part of the assessment?	Yes to internal penetration test and wireless subnet. No to telephony/IT phones.
48	Our assumption in section 3.3 is this is an assessment of the Data Center only. Is this correct?	This is will of the County Data Network plus one Subdomain.
49	Is there a prioritized list of application that will be given as part of section 3.4? Are you going to provide a list of applications and IP address that you want tested?	We will provide a prioritized list if needed during the contract negotiation. Yes, during contract negotiations.
50	Is this a system compliance analysis or would you also like a process compliance review as part of section 3.5 and 3.6? If a process compliance is require, access to applications and environments outside of the data center would need to be made available as part of the assessment. For a system compliance analysis of sections 3.5 and 3.6, are black box reports sufficient or is something more specific required? Is this in preparation of a full audit?	No, not during this testing, however it will be an option on a time material basis after the 5/31/2016 delivery requirement.
51	Please explain or expand on your desire of a Forensics analysis in section 3.7.3.	We would like to understand the tools, techniques and findings thus are requiring the items listed.
52	Are there critical systems that are off limits for testing? Are there ideal or limited times for penetration testing?	We do not, however prefer off-hours and avoidance of back-up window.
53	We generally provide a Certificate of Insurance that shows we have appropriate coverage, however we do not customize these certificates until an award is imminent. Therefore, we were not planning on creating a 'Franklin County' specific document for this proposal response. Please confirm this is acceptable.	That is acceptable.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
54	Will Franklin County consider an extension on the January 22nd , 2PM RFQ submittal due date?	The FCDC will not consider an extension of the January 22 at 2 p.m. RFQ submittal date as a result of our deadline for final deliverable submission no later than May 31, 2016.
55	What components of HIPAA compliance is Franklin County looking to assess – Meaningful Use, Security Rule, Privacy Rule, security of Business Associates?	Security rules, privacy rules, security and business associates.
56	Are the core data center located in a campus environment or are their satellite locations more than 2 miles away?	Satellites for the network. All applications chosen are within the campus.
47	Is the FCDN generally well-connected or are their bandwidth limitations at any of the 25 locations?	450 mbps.
58	How many significant network egress points are there from the FCDC? Does Franklin County maintain network taps at the three identified layers (Intranet, DMZ, Outside) or does it have sufficient port density to permit taps to examine traffic?	We have 5 egress points. Yes.
59	Does Franklin County desire on-site/internal penetration testing to include wireless?	Yes.
60	What is the approximate number of active IPs for Franklin County FCDN – is the current scope generally within 198.30.0.0/16?	Approximately 16,777,214 IP addresses available internal and 2500 available external IP addresses, not all of them are used.
61	Is Franklin County using this assessment as part of their official PCI compliance program reporting?	No.
62	Does Franklin County support the use of sampling methodologies to control engagement costs?	Yes.
63	Will Franklin County require assistance for remediation/mitigation tasks?	Recommendations are part of this RFQ and the optional hourly cost might be utilized for remediation and mitigation.
64	Does Franklin County currently follow any IT management or security framework such as ITIL or ISO?	No.
65	Is there an incumbent?	We do not have someone preselected to do this work nor are we currently working with a vendor.
66	Section 3.0: • How many systems and IP subnets does the County anticipate being assessed? o Internal o External o DMZ	Approximately 16,777,214 IP addresses available internal and 2500 available external IP addresses, not all of them are used.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
67	RFQ section 3.2 (p. 32)"Ethical hack and penetration testing" and the notes in Section 3.0 (p. 33) "Any and all penetration testing performed to assess vulnerabilities must be non-invasive, …" • Should an exploitable vulnerability be identified? • Is it the County's desire for the Vendor to conduct privilege escalation and related activities to identify potential avenues of increased privilege access? • For example, a vulnerability on an external web server is identified that grants the Vendor's team full remote access. Should the team utilize this vulnerability and attempt to gain additional access to internal systems?	Yes, Yes.
68	RFQ section 3.3.2 (p. 32) "All wired and wireless devices, including but not limited to…" • Is the County requesting the Vendor perform a security assessment of the County's wireless network? • If so, does the Vendor need to perform a walk-through of all County facilities were wireless access is provided or will the County provide a representative sample for the Vendor? • If the County is requesting a wireless security assessment, should the Vendor attempt to penetrate the wireless network? This includes attempting to crack wireless encryption and bypass any authentication mechanisms employed.	Yes and only for selected locations, we would like to have recommendation from vendor, yes.
69	RFQ section 3.3.5 (p. 32) "One 2-way trusted domain with the FCDC" • Should this 'trusted domain' (its servers, systems, networks) be assessed, or should this only consist of a review of the domain trust relationship? • Does Franklin County own this domain? • If not, will Franklin County obtain the appropriate permissions to allow the vendor to conduct security assessments and penetration tests of the trusted domain?	Yes, yes.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
70	RFQ section 3.4.3 (p. 32) "One third-party software application" • Is this third-party software application controlled and operated by the County? • Is it hosted in the County's network/IP space? • If not, will the County ensure that relevant permissions are obtained from the system/program owner for testing?	Yes, yes, not a cloud app.
71	RFQ section 3.5 (p. 32) "Assessment, HIPAA (Health Insurance Portability and Accountability Act) compliance" • Does the County have a specific list of assets (networks, systems, or programs) that should be assessed for HIPAA compliance? • How many systems and IP subnets are included in this assessment phase?	Yes, and no more than five
72	RFQ section 7.1 (p. 36) "Work Hours" • Does the County anticipate requiring ALL work be conducted at FCDC offices? • Does the County anticipate that some work, such as external vulnerability assessments and penetration tests, may be conducted remotely? • How many facilities does the County anticipate the Vendor will need to work from?	No, yes, between 3-5.
73	Appendix D (p. 27)," Appendix D references "Worker's Compensation Liability Certificate Requirements, however, Section 10.04 covers Non-Collusion certificate. Will this this discrepancy be corrected?	Yes, refer to Amendment 1.
74	In regards to Appendix D (p. 27), "Worker's Compensation Liability Certificate": Appendix D states that 1 original and 7 copies of this certificate must be submitted with the proposal. Administrative Section 10.03 requires the awarded contractor to provide the certificate after notification of award. Will the county please clarify as to if this certificate is required as part of the Proposal at time of submission? Question not needed. This happens both time the COI for the proposal is not the same as for the awarded contract	The awarded Contractor will be required to provide said Cerfificate within seven (7) calendar days after notification to award.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
75	Appendix D (p. 27), "Appendix E - Pricing Appendix D states Appendix E has been released in Microsoft Excel format in the Franklin County Purchasing Department Website. However, the Appendix is missing, When will the county release Appendix E on the Website?	Refer to Amendment 1.
76	5.6 Cost Summary (p. 35) 5.6 Cost summary references "Section 8.0 below." We are unable to find the reference Section 8.0 in the document. Will the county please clarify? Should this be Appendix E?	Refer to Amendment 1.
77	section 3.6 (p.32) "Assessment PCI (Payment Card Industry) compliance" • Does the County have a specific list of assets (networks, systems, or programs) that should be assessed for PCI compliance? • Does the County require, as part of the response, that the Vendor be PCI Qualified Security Assessor (QSA)-Certified? • How many systems and IP subnets are included in this assessment phase?	No, yes, no more than five.
78	On Page 6 of the PDF, in 1.10 it states no changes are allowed. Also see Page 34, in Section 5.5 of the Request for Qualifications page 34 of 42, this language is contrary to the language of 1.10 just mentioned. What is actually allowed?	All assumptions made by the vendor in preparing the proposal shall be stated. If the vendor is making any exception to an item or provision it must be clearly stated than will be discussed during/ if chosen - final interview and contract negotiation.
79	On Page 14 of the PDF, in 5.01 it states that the awarded contract will be for a period of one-year, beginning February 23, 2016 through May 31, 2016. On page 9, in 2.14 it states that Offeror to produce deliverables by May 31, 2016. On Pages 33-34, Section 4.0, it implies that work and reports need to be completed within 7 weeks of PO receipt, with Final Oral Presentation by May 31, 2016. Which timeline should be considered the baseline? Is there additional work that would extend the contract work to the one year term as indicated in 5.01?	We will enter into a one-year contract even though the deliverable is due 5/31/2016 because there is also an option for additional services on an hourly basis.
80	Where do we find the Microsoft Excel Cost Schedule spreadsheet on the Franklin County Purchasing Department website?	Refer to Amendment 1.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
81	On Page 31 of the PDF, in Section 2.0, it states that there are 25 locations. On Page 32, in Section 3.3, it states that all components of the FCDN must be assessed. Later in Section 3.3.5, it states One Sub-Domain and in Section 3.36 End-point devices. Is the expectation that an assessment will be conducted across the entire FCDN, or a selected sub-domain with its included devices, plus the application layer assessments of Section 3.4? Will we be able to access the full FCDN from one location with firewall rule changes?	This will include a scan of the FCDN network and a deeper comprehensive assessment of one subdomain.
82	As the FCDN is a multi-tenant environment, will be have a POC who can approve testing in a timely fashion?	Yes, you will have a POC for each area and approval within 24 hours.
83	Is there a standard weekly status report template that we will be required to use?	No - your report will be approved during contract negotiations.
84	On Page 27, Appendix D, Administrative Requirements indicate Sections 11.02 and 11.05. Is this to be 11.06 and 11.09?	Refer to Amendment 1.
85	On Page 27, Appendix D, Insurance Certificate. Will a full original additional insured certificate be necessary before contract award?	No, this will be done during contract negotiations.
86	Will we be able to ask additional simple form submittal questions after today?	No.
87	Ref. General Information, Certificate of Good Standing As an out-of-state corporation, where do we include a copy of our Certificate of Good Standing from the state of our incorporation in our bid response? Please clarify.	Yes.
88	Ref. Administrative Requirements, Section 1.06 Registration with Franklin County Does a bidder need to register with Franklin County prior to the bid submission date of January 22, 2016? Please clarify.	Yes.
90	Ref. Section 5.0 Requirements Under 5.2 Company Qualifications, the request is made for client references. Does a vendor submit Appendix B in this section? Please clarify.	No, please utilize appendix B for references and qualifications within the RFQ response.
91	Ref. Section 5.0 Requirements a. Under 5.4 Key Personnel and Roles, the request is made to …show proof of security checks. Please clarify the types of security checks required and the proof required.	A statement of the vendors policy for security checks.
92	Is there a preferred Risk evaluation approach that will need to be considered for the engagement? If yes, please elaborate.	No, we would like you to advise what your risk approach would be.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
93	Would all assessing and testing as part of this request take place at a single physical location?	No.
94	How many locations leverage wireless technology?	15
95	Would off-site internal network scanning be agreeable in order to reduce costs?	If it does not require us to alter the firewall, that would be permitted - we are looking for vendor recommendations.
96	Will penetration testing be allowed during business hours?	With all but one application described in section 3.3.3.
97	Are there any internal security standards that devices, systems, processes or applications should be compared against for this overall assessment?	Internal policy.
98	Does FCDC have at least one network segment that is authorized to access all other internal and DMZ network segments for testing purposes?	No .
99	Do you utilized any virtualization technologies that would support either your end devices or Windows domain servers?	End Device - No. Windows, yes.
100	What type of end-point devices does FCDC deploy and manage?	PC computers, printers, mobile devices, scanners.
101	Are FCDC managed database, such as Microsoft SQL or Oracle, a part of the in-house developed Windows based application or IBM iSeries integrated applications?	SQL and DB2.
102	What is the total number IP Addresses/hosts (Internet Accessible) that will be in scope for the assessment?	Approximately 16,777,214 IP addresses available internal and 2500 available external IP addresses, not all of them are used.
103	Will the web application assessment be unauthenticated (no credentials provided for testing) or is your preference to have testing performed as an authenticated person?	Both. Black Box - then we will provide standard user credential.
104	Is the web application to be in-scope, owned and hosted by FCDC?	Yes.
105	What is the anticipated in-scope web application developed in (the type of coding used)?	Cold Fusion and Microsoft SQL Server.
106	Approximately how many dynamic pages are within the anticipated in-scope web application?	6 pages.
107	How many different user levels/roles are there within the in-scope web application?	1 role.
108	Have you already completed a Self-Assessment Questionnaire for PCI; are you able to share your average type and amount of transactions you process?	No. Transactions per year are less than 100,000.
109	Can you elaborate on the Forensic analysis and artifacts subsection 3.7.3 documentation requirement? What forensic events are you anticipating as part of the scope of this review?	We would like to understand the tools, techniques and findings thus are requiring the items listed.

Franklin County RFQ 2016-22-02 Questions and Answers

#	Question	Response
110	Is the requested HIPAA assessment to serve as a gap assessment or an actual evaluation to the security rule, breach notification, privacy rule (or all three)?	Actual evaluation and all three.
111	Can FCDC able to share the number of applications, departments whom own, process, transmit, or modify protected health information?	This information will be provided during contract negotiation.
112	Has FCDC previously performed a HIPAA Risk Assessment? If so, is this something you are able to share?	No.
113	Can FCDC share how many third parties and Business Associates exist, whom interact with protected health information?	No.
114	In Appendix D: Offeror Deliverables Checklist, it is mentioned that Appendix E – Pricing Forms has been released in .xls format on the Franklin County Purchasing Department website, however it does not appear to be with the other documents on the page for this RFQ. We would appreciate your assistance with obtaining Appendix E – Pricing forms in .xls format.	Refer to Amendment 1.